EXPRESS MAIL NO. EV 078 052 260

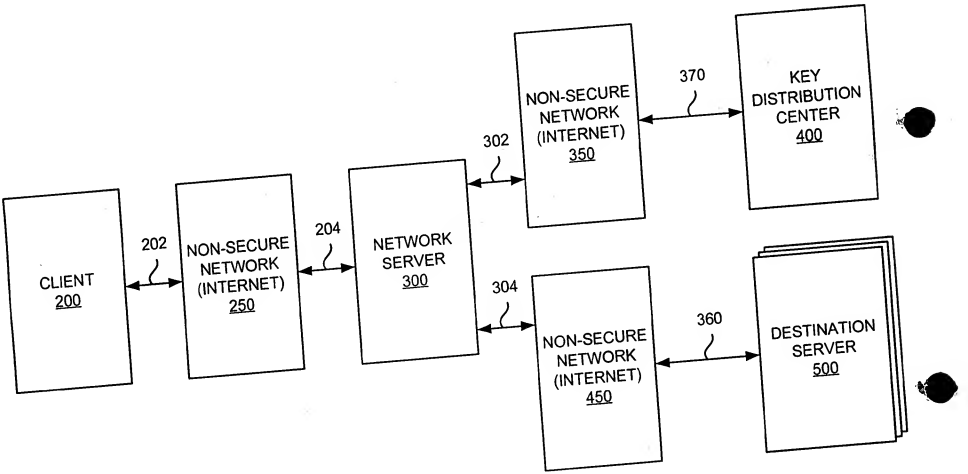


FIGURE 1

EXPRESS MAIL NO. EL 652760

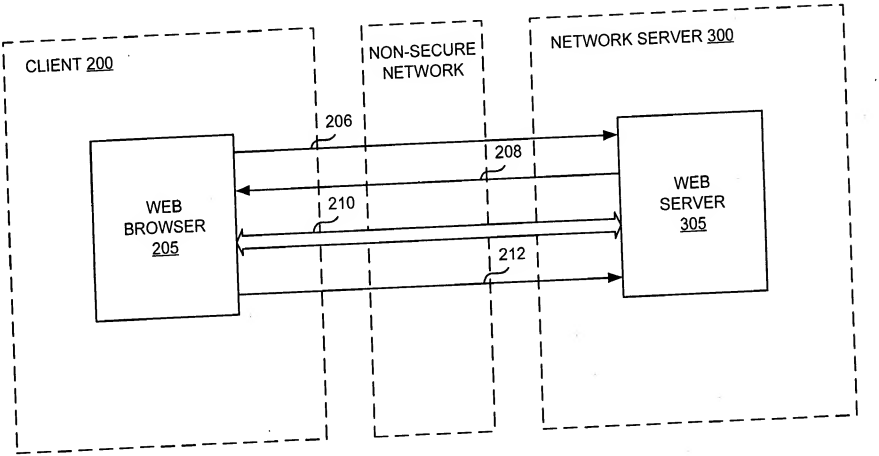


FIGURE 2

10210 00165260

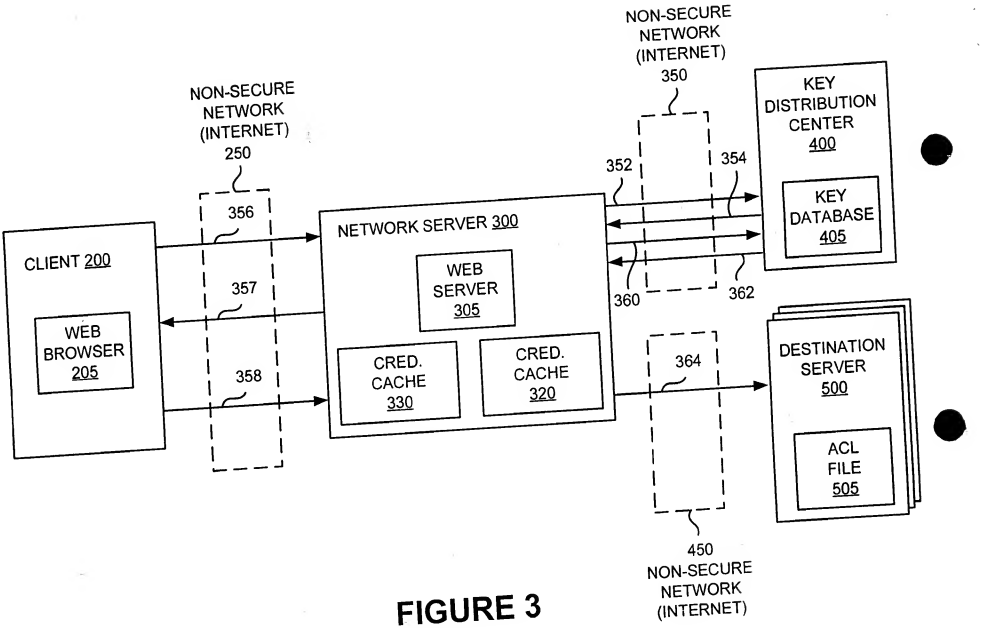


FIGURE 3

TUCITU 00105260

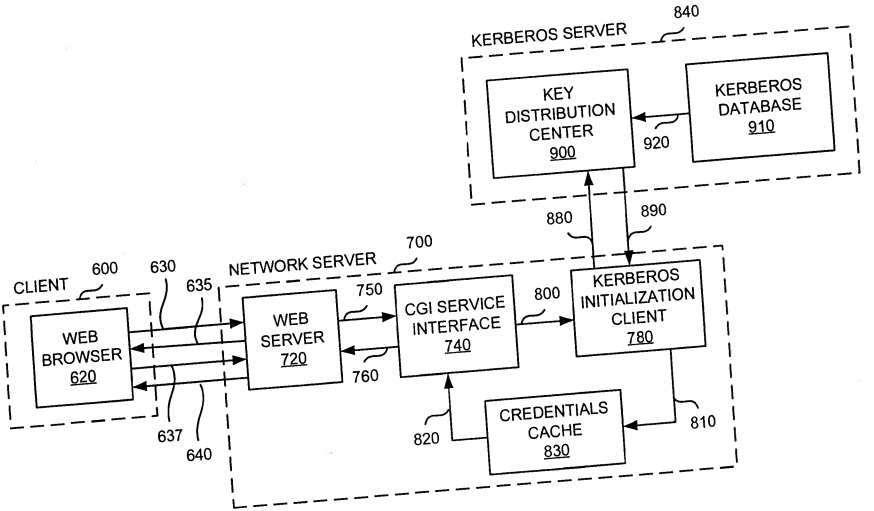


FIGURE 4

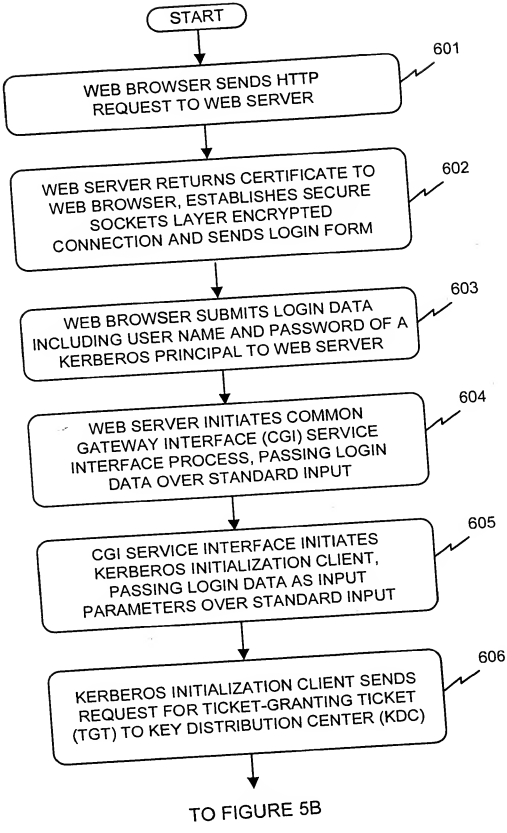

START
601
WEB BROWSER SENDS HTTP REQUEST TO WEB SERVER
602
WEB SERVER RETURNS CERTIFICATE TO WEB BROWSER, ESTABLISHES SECURE SOCKETS LAYER ENCRYPTED CONNECTION AND SENDS LOGIN FORM
603
WEB BROWSER SUBMITS LOGIN DATA INCLUDING USER NAME AND PASSWORD OF A KERBEROS PRINCIPAL TO WEB SERVER
604
WEB SERVER INITIATES COMMON GATEWAY INTERFACE (CGI) SERVICE INTERFACE PROCESS, PASSING LOGIN DATA OVER STANDARD INPUT
605
CGI SERVICE INTERFACE INITIATES KERBEROS INITIALIZATION CLIENT, PASSING LOGIN DATA AS INPUT PARAMETERS OVER STANDARD INPUT
606
KERBEROS INITIALIZATION CLIENT SENDS REQUEST FOR TICKET-GRANTING TICKET (TGT) TO KEY DISTRIBUTION CENTER (KDC)
TO FIGURE 5B

FIGURE 5A

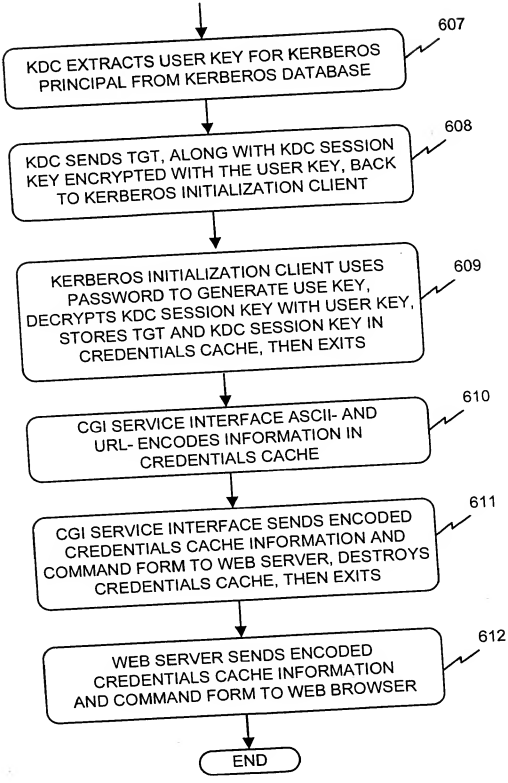
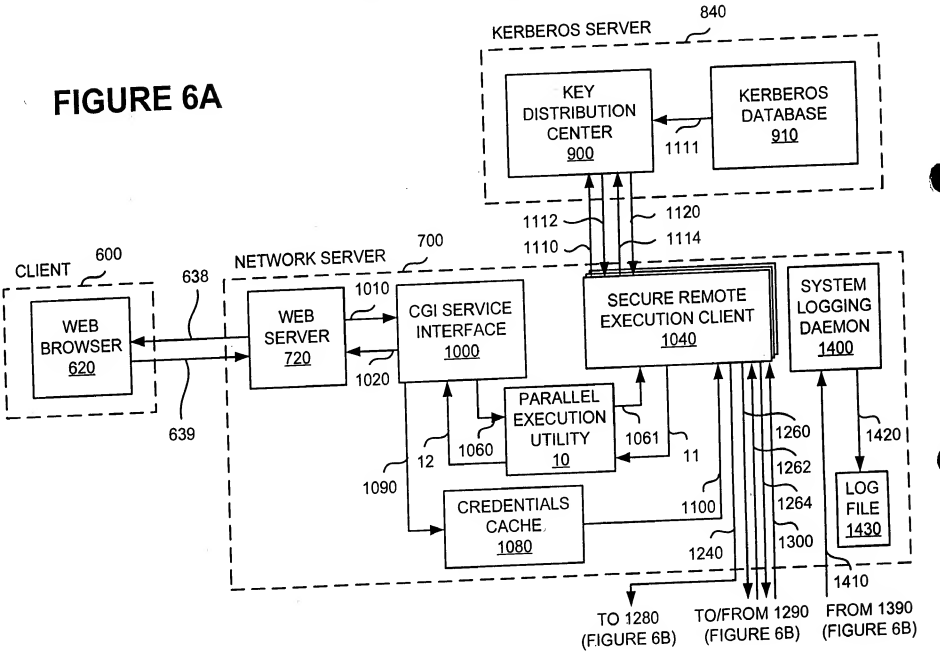

FROM FIGURE 5A
607
KDC EXTRACTS USER KEY FOR KERBEROS PRINCIPAL FROM KERBEROS DATABASE
608
KDC SENDS TGT, ALONG WITH KDC SESSION KEY ENCRYPTED WITH THE USER KEY, BACK TO KERBEROS INITIALIZATION CLIENT
609
KERBEROS INITIALIZATION CLIENT USES PASSWORD TO GENERATE USE KEY, DECRYPTS KDC SESSION KEY WITH USER KEY, STORES TGT AND KDC SESSION KEY IN CREDENTIALS CACHE, THEN EXITS
610
CGI SERVICE INTERFACE ASCII- AND URL- ENCODES INFORMATION IN CREDENTIALS CACHE
611
CGI SERVICE INTERFACE SENDS ENCODED CREDENTIALS CACHE INFORMATION AND COMMAND FORM TO WEB SERVER, DESTROYS CREDENTIALS CACHE, THEN EXITS
612
WEB SERVER SENDS ENCODED CREDENTIALS CACHE INFORMATION AND COMMAND FORM TO WEB BROWSER
END

FIGURE 5B

PCT/US00/05260

FIGURE 6A



Tue, 10 Oct 2006 09:26:50

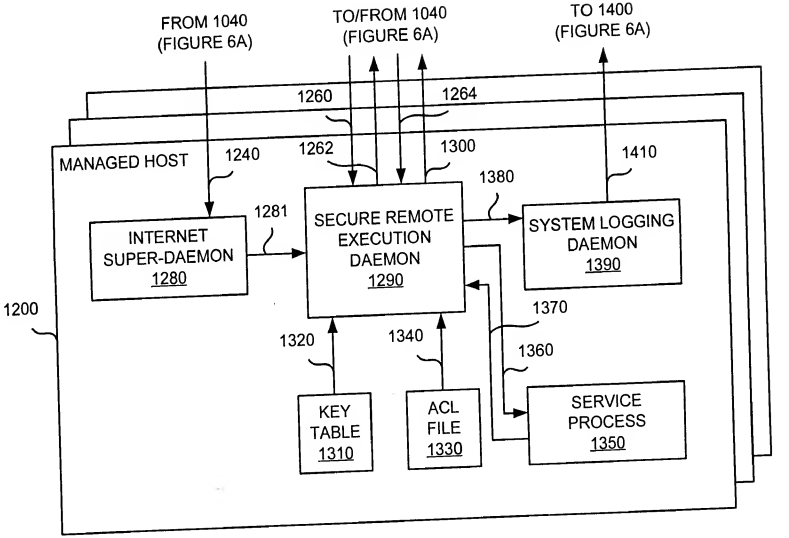


FIGURE 6B

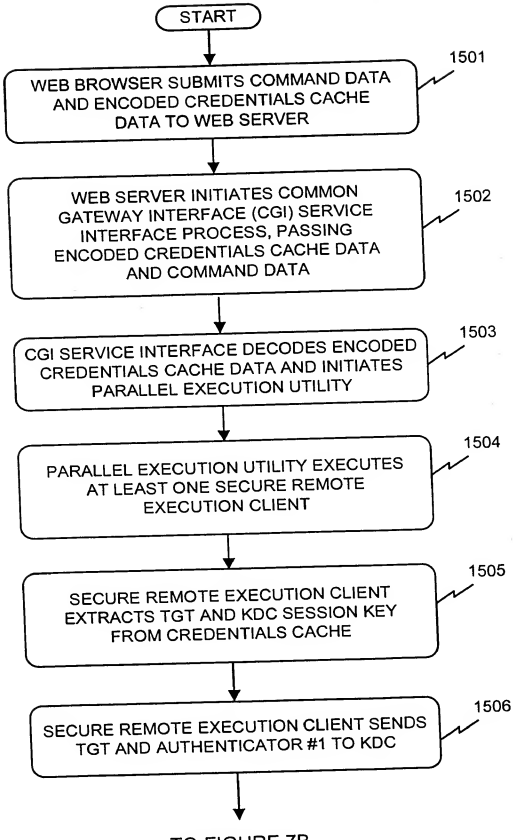

START
WEB BROWSER SUBMITS COMMAND DATA AND ENCODED CREDENTIALS CACHE DATA TO WEB SERVER
1501
WEB SERVER INITIATES COMMON GATEWAY INTERFACE (CGI) SERVICE INTERFACE PROCESS, PASSING ENCODED CREDENTIALS CACHE DATA AND COMMAND DATA
1502
CGI SERVICE INTERFACE DECODES ENCODED CREDENTIALS CACHE DATA AND INITIATES PARALLEL EXECUTION UTILITY
1503
PARALLEL EXECUTION UTILITY EXECUTES AT LEAST ONE SECURE REMOTE EXECUTION CLIENT
1504
SECURE REMOTE EXECUTION CLIENT EXTRACTS TGT AND KDC SESSION KEY FROM CREDENTIALS CACHE
1505
SECURE REMOTE EXECUTION CLIENT SENDS TGT AND AUTHENTICATOR #1 TO KDC
1506
TO FIGURE 7B

FIGURE 7A

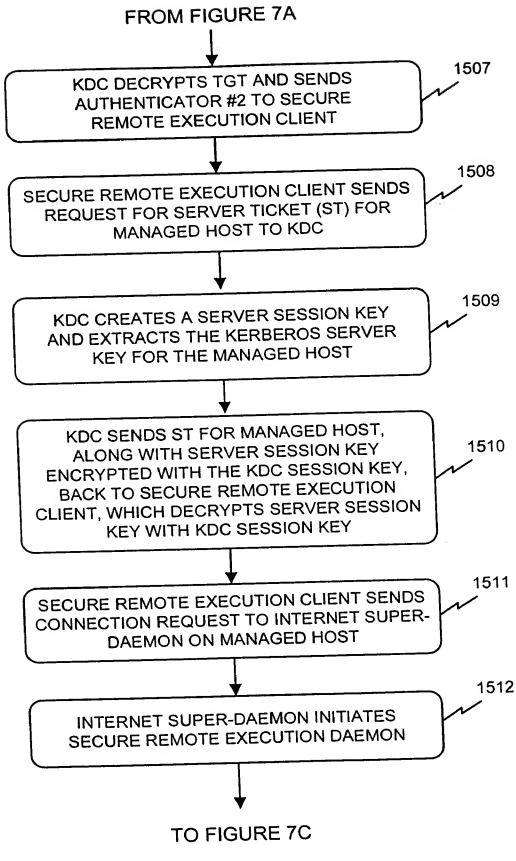

FROM FIGURE 7A
KDC DECRYPTS TGT AND SENDS AUTHENTICATOR #2 TO SECURE REMOTE EXECUTION CLIENT
1507
SECURE REMOTE EXECUTION CLIENT SENDS REQUEST FOR SERVER TICKET (ST) FOR MANAGED HOST TO KDC
1508
KDC CREATES A SERVER SESSION KEY AND EXTRACTS THE KERBEROS SERVER KEY FOR THE MANAGED HOST
1509
KDC SENDS ST FOR MANAGED HOST, ALONG WITH SERVER SESSION KEY ENCRYPTED WITH THE KDC SESSION KEY, BACK TO SECURE REMOTE EXECUTION CLIENT, WHICH DECRYPTS SERVER SESSION KEY WITH KDC SESSION KEY
1510
SECURE REMOTE EXECUTION CLIENT SENDS CONNECTION REQUEST TO INTERNET SUPER-DAEMON ON MANAGED HOST
1511
INTERNET SUPER-DAEMON INITIATES SECURE REMOTE EXECUTION DAEMON
1512
TO FIGURE 7C

FIGURE 7B

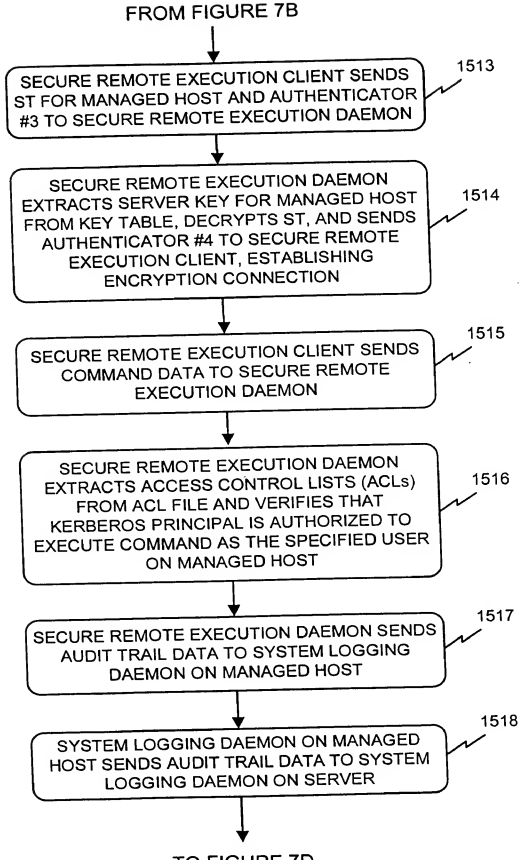

FROM FIGURE 7B
SECURE REMOTE EXECUTION CLIENT SENDS ST FOR MANAGED HOST AND AUTHENTICATOR #3 TO SECURE REMOTE EXECUTION DAEMON
1513
SECURE REMOTE EXECUTION DAEMON EXTRACTS SERVER KEY FOR MANAGED HOST FROM KEY TABLE, DECRYPTS ST, AND SENDS AUTHENTICATOR #4 TO SECURE REMOTE EXECUTION CLIENT, ESTABLISHING ENCRYPTION CONNECTION
1514
SECURE REMOTE EXECUTION CLIENT SENDS COMMAND DATA TO SECURE REMOTE EXECUTION DAEMON
1515
SECURE REMOTE EXECUTION DAEMON EXTRACTS ACCESS CONTROL LISTS (ACLs) FROM ACL FILE AND VERIFIES THAT KERBEROS PRINCIPAL IS AUTHORIZED TO EXECUTE COMMAND AS THE SPECIFIED USER ON MANAGED HOST
1516
SECURE REMOTE EXECUTION DAEMON SENDS AUDIT TRAIL DATA TO SYSTEM LOGGING DAEMON ON MANAGED HOST
1517
SYSTEM LOGGING DAEMON ON MANAGED HOST SENDS AUDIT TRAIL DATA TO SYSTEM LOGGING DAEMON ON SERVER
1518
TO FIGURE 7D

FIGURE 7C

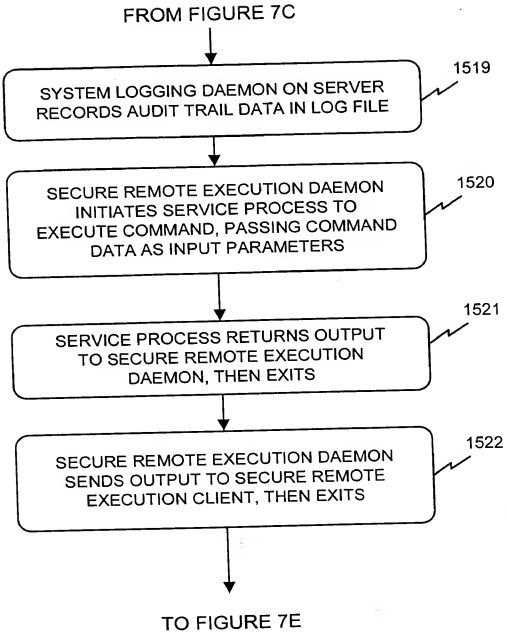

FROM FIGURE 7C
SYSTEM LOGGING DAEMON ON SERVER RECORDS AUDIT TRAIL DATA IN LOG FILE
1519
SECURE REMOTE EXECUTION DAEMON INITIATES SERVICE PROCESS TO EXECUTE COMMAND, PASSING COMMAND DATA AS INPUT PARAMETERS
1520
SERVICE PROCESS RETURNS OUTPUT TO SECURE REMOTE EXECUTION DAEMON, THEN EXITS
1521
SECURE REMOTE EXECUTION DAEMON SENDS OUTPUT TO SECURE REMOTE EXECUTION CLIENT, THEN EXITS
1522
TO FIGURE 7E

FIGURE 7D

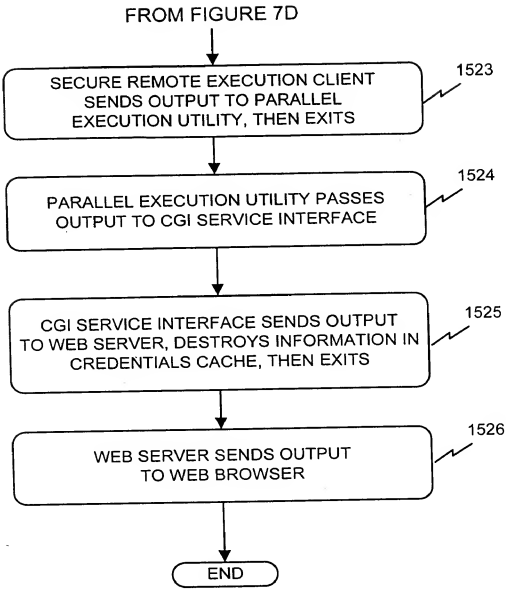
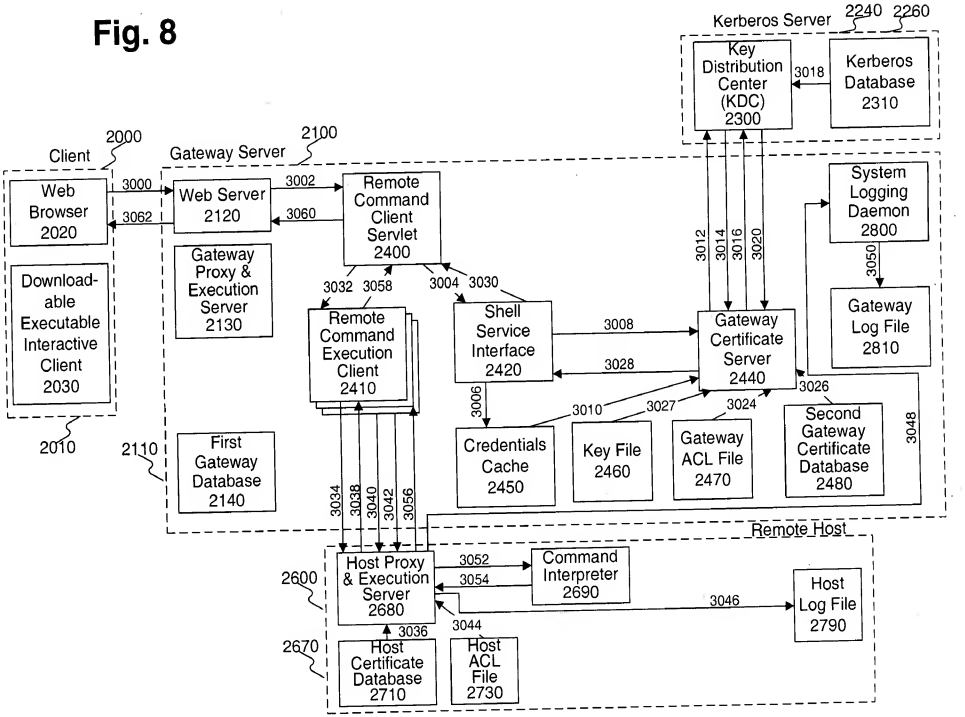

FROM FIGURE 7D
SECURE REMOTE EXECUTION CLIENT SENDS OUTPUT TO PARALLEL EXECUTION UTILITY, THEN EXITS
1523
PARALLEL EXECUTION UTILITY PASSES OUTPUT TO CGI SERVICE INTERFACE
1524
CGI SERVICE INTERFACE SENDS OUTPUT TO WEB SERVER, DESTROYS INFORMATION IN CREDENTIALS CACHE, THEN EXITS
1525
WEB SERVER SENDS OUTPUT TO WEB BROWSER
1526
END

FIGURE 7E

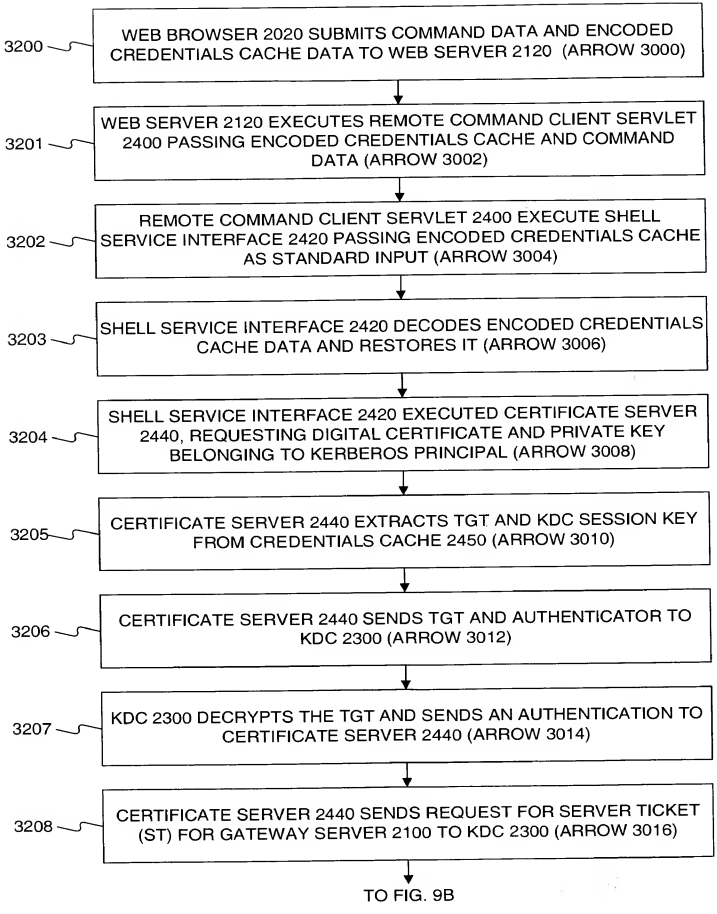
Docket 001652.00

Fig. 8



Attorney Docket No. 42390.P4204

FIG. 9A



7021403-0005760

FIG. 9B

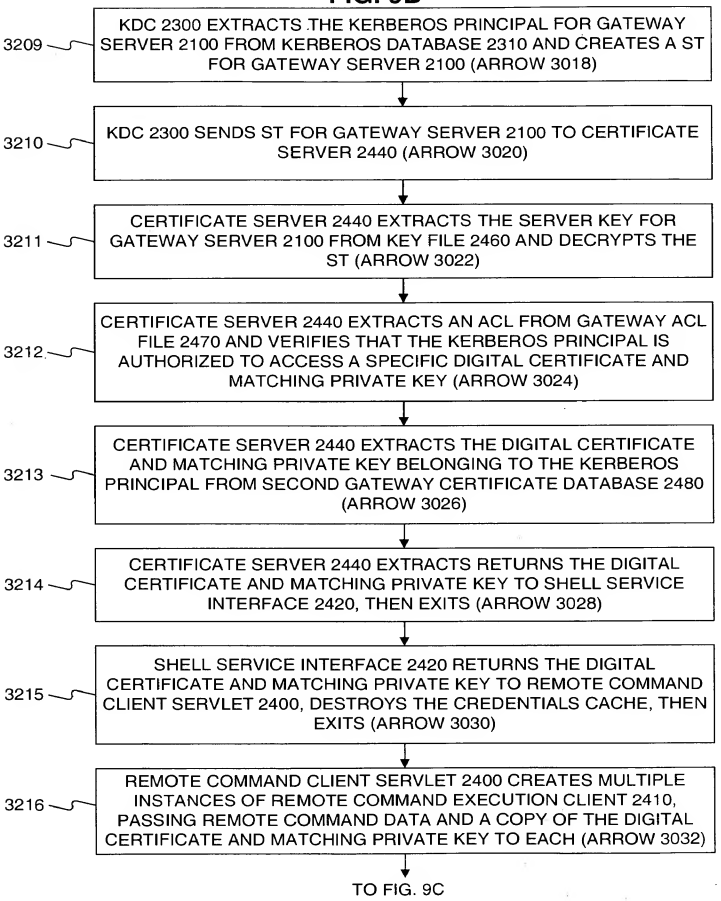


Exhibit 1005

FIG. 9C

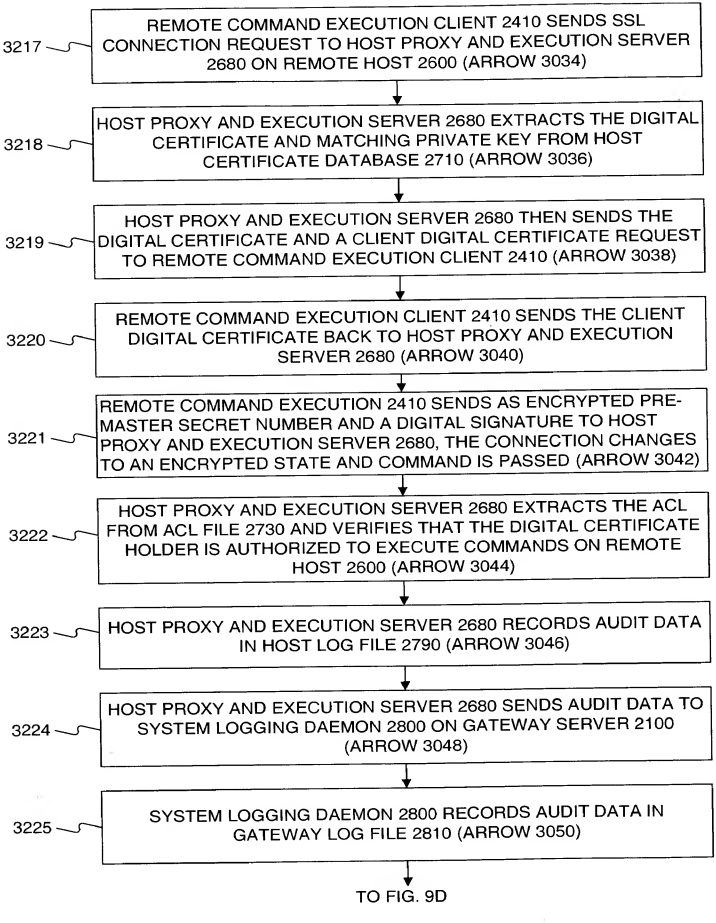


FIG. 9D

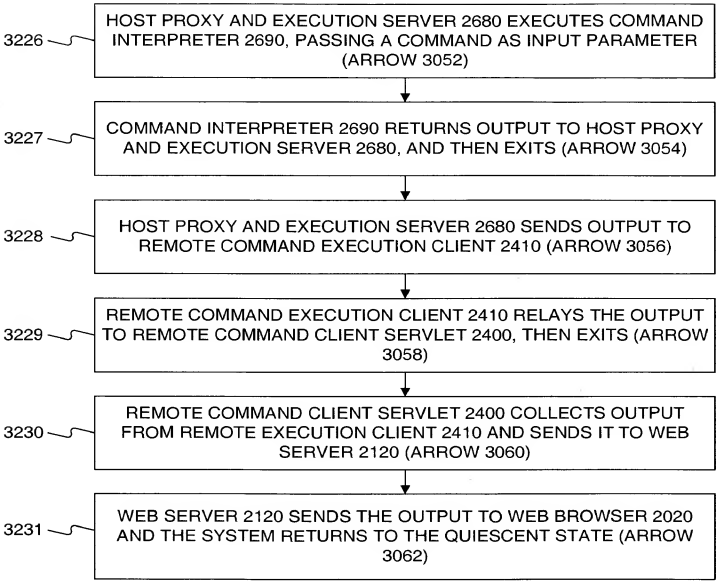

3226
HOST PROXY AND EXECUTION SERVER 2680 EXECUTES COMMAND INTERPRETER 2690, PASSING A COMMAND AS INPUT PARAMETER (ARROW 3052)
3227
COMMAND INTERPRETER 2690 RETURNS OUTPUT TO HOST PROXY AND EXECUTION SERVER 2680, AND THEN EXITS (ARROW 3054)
3228
HOST PROXY AND EXECUTION SERVER 2680 SENDS OUTPUT TO REMOTE COMMAND EXECUTION CLIENT 2410 (ARROW 3056)
3229
REMOTE COMMAND EXECUTION CLIENT 2410 RELAYS THE OUTPUT TO REMOTE COMMAND CLIENT SERVLET 2400, THEN EXITS (ARROW 3058)
3230
REMOTE COMMAND CLIENT SERVLET 2400 COLLECTS OUTPUT FROM REMOTE EXECUTION CLIENT 2410 AND SENDS IT TO WEB SERVER 2120 (ARROW 3060)
3231
WEB SERVER 2120 SENDS THE OUTPUT TO WEB BROWSER 2020 AND THE SYSTEM RETURNS TO THE QUIESCENT STATE (ARROW 3062)

Fig. 10

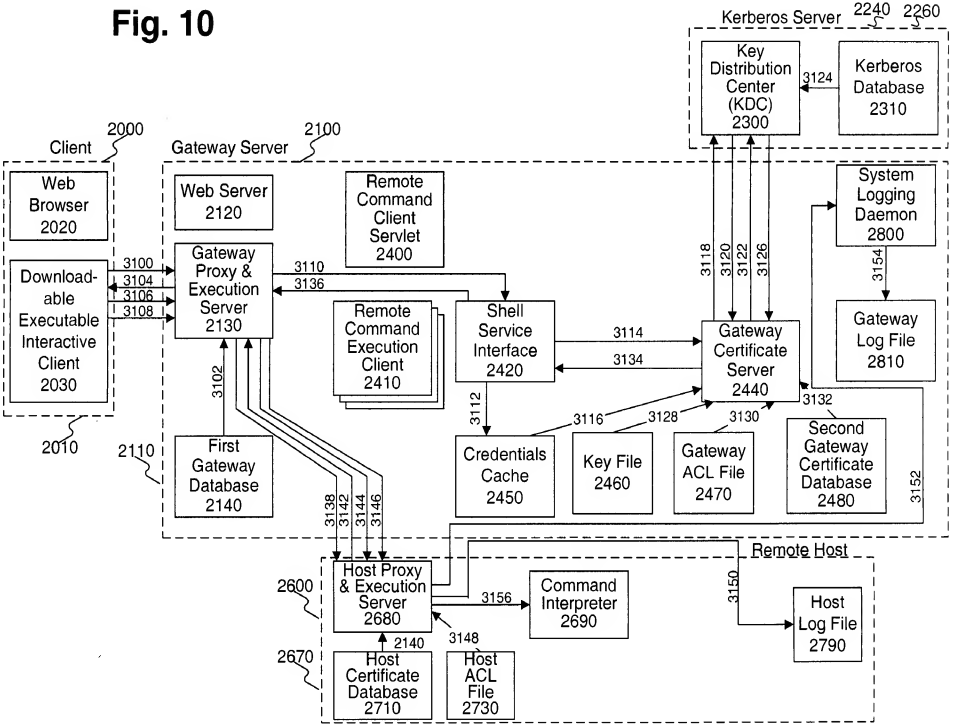
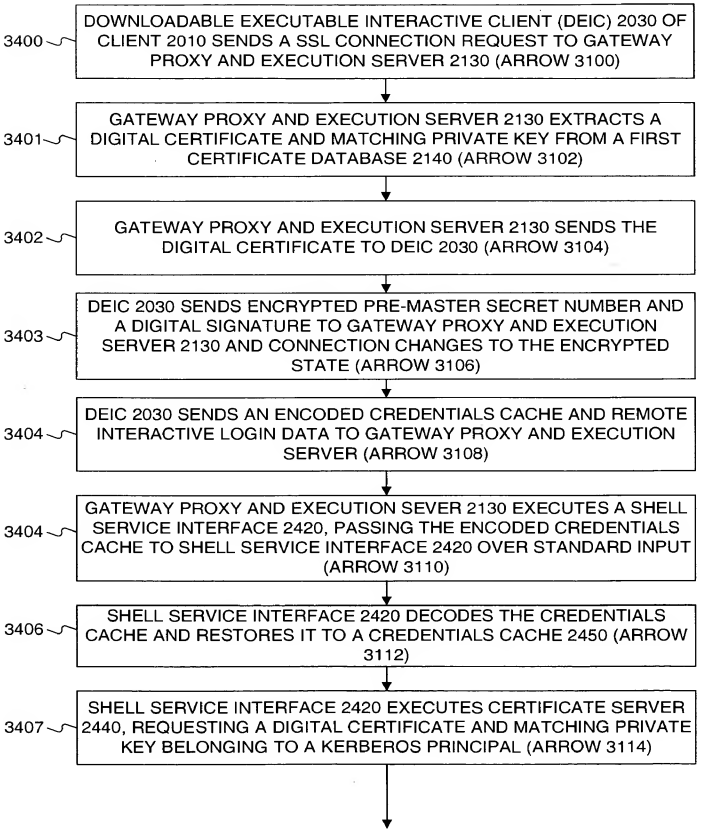
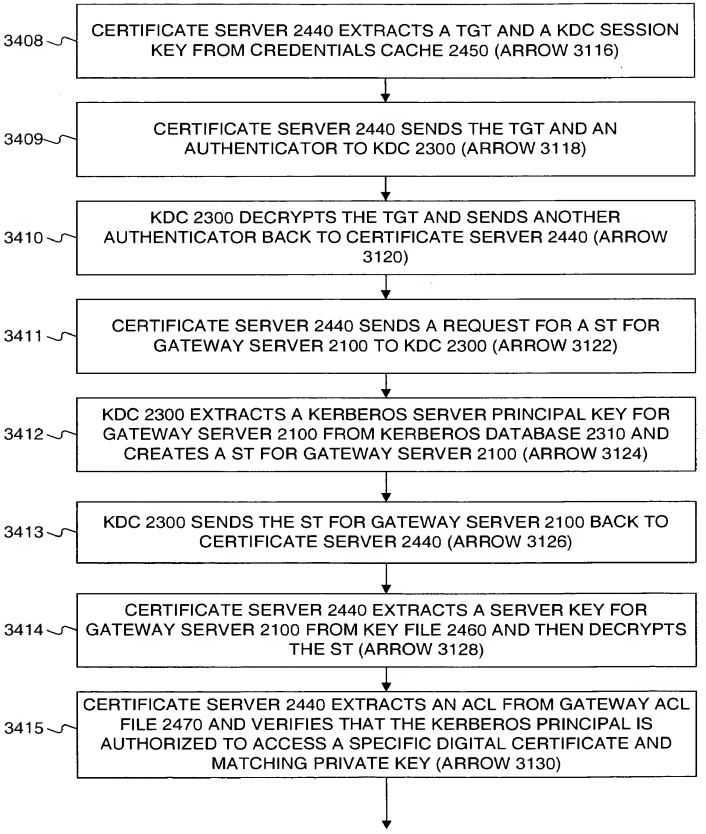

Kerberos Server
2240
2260
Key Distribution Center (KDC) 2300
3124
Kerberos Database 2310
Client
2000
Gateway Server
2100
Web Browser 2020
Web Server 2120
Remote Command Client Servlet 2400
System Logging Daemon 2800
Downloadable Executable Interactive Client 2030
3100
3104
3106
3108
Gateway Proxy & Execution Server 2130
3110
3136
3118
3120
3122
3126
3154
Remote Command Execution Client 2410
Shell Service Interface 2420
3114
3134
Gateway Certificate Server 2440
Gateway Log File 2810
3102
3112
3116
3128
3130
3132
2010
2110
First Gateway Database 2140
Credentials Cache 2450
Key File 2460
Gateway ACL File 2470
Second Gateway Certificate Database 2480
3152
3138
3142
3144
3146
Remote Host
2600
Host Proxy & Execution Server 2680
3156
Command Interpreter 2690
3150
Host Log File 2790
2140
3148
2670
Host Certificate Database 2710
Host ACL File 2730

FIG. 11A



TO FIG. 11B

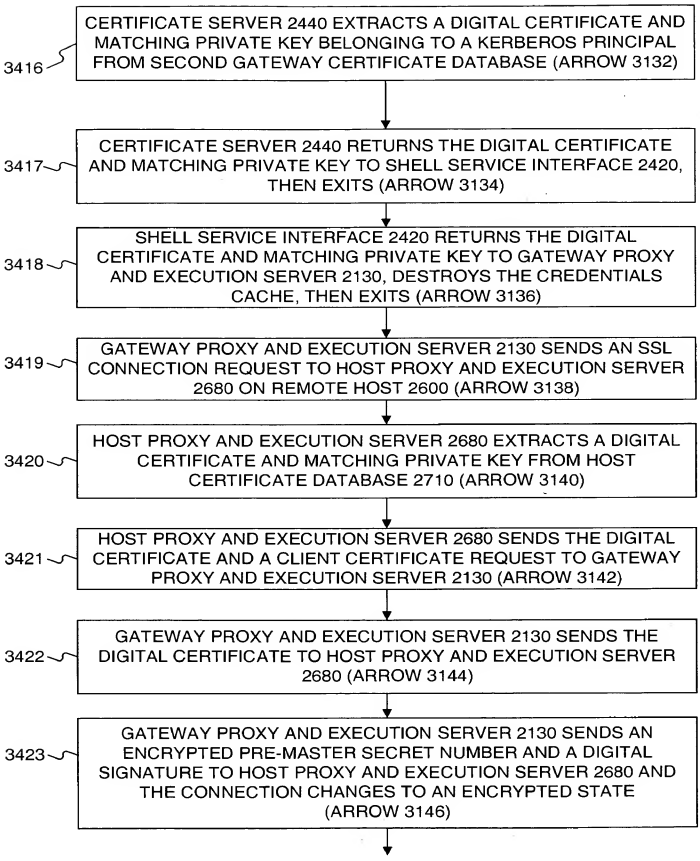
FIG. 11B



TO FIG. 11C

Docket No. 50277-0011

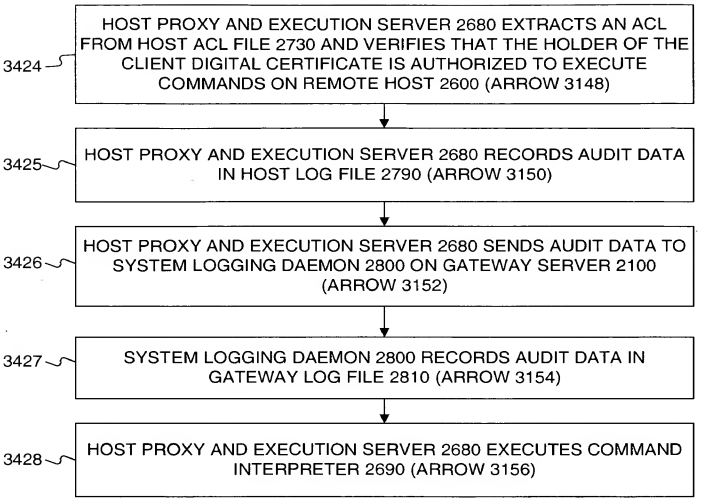
FIG. 11C



TO FIG. 11D

EXHIBIT 1002

FIG. 11D


3424
HOST PROXY AND EXECUTION SERVER 2680 EXTRACTS AN ACL FROM HOST ACL FILE 2730 AND VERIFIES THAT THE HOLDER OF THE CLIENT DIGITAL CERTIFICATE IS AUTHORIZED TO EXECUTE COMMANDS ON REMOTE HOST 2600 (ARROW 3148)
3425
HOST PROXY AND EXECUTION SERVER 2680 RECORDS AUDIT DATA IN HOST LOG FILE 2790 (ARROW 3150)
3426
HOST PROXY AND EXECUTION SERVER 2680 SENDS AUDIT DATA TO SYSTEM LOGGING DAEMON 2800 ON GATEWAY SERVER 2100 (ARROW 3152)
3427
SYSTEM LOGGING DAEMON 2800 RECORDS AUDIT DATA IN GATEWAY LOG FILE 2810 (ARROW 3154)
3428
HOST PROXY AND EXECUTION SERVER 2680 EXECUTES COMMAND INTERPRETER 2690 (ARROW 3156)